REMARKS

Applicant has studied the Office Action dated June 3, 2004 and has made amendments to the claims. It is submitted that the application, as amended, is in condition for allowance. Claims 1-24 are pending. Claims 1, 2, 4-10, 13-15, 17-19, and 21-23 have been amended. Reconsideration and allowance of the claims in view of the above amendments and the following remarks are respectfully requested.

As an initial matter, Applicant notes that the present Office Action specified that the "SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 6 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION." Thus, the due date for responding to the present Office Action is December 3, 2004. Accordingly, Applicant submits that this reply can be filed without the need for an extension of time. However, if it should be determined that an extension of time is required to prevent this application from becoming abandoned, or for any other reason an insufficient fee has been paid, please charge any insufficiency to Deposit Account No. 50-1556.

Claims 1, 2, 14, 15, 22, and 23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Pfab (U.S. Patent No. 6,195,752). Claims 3-13, 16-21, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Pfab in view of Menezes et al. ("Book of Applied Cryptography," pp. 10, 51, 64).[1] These rejections are respectfully traversed.

The present invention is directed to methods and circuits for transferring data in a highly secure manner. One preferred embodiment provides a method for secured transfer of an N-byte data element from a first memory containing the data element to a second memory through a data

---

[1] While the Office Action states that claims 3-13, 16-21, and 24 were "rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes," Applicant believes based on the Examiner's reasoning with respect to these dependent claims that these claims were actually rejected under 35 U.S.C. § 103(a) as being unpatentable over Pfab in view of Menezes.

bus that is connected between the first memory and the second memory. According to the method, the value of at least one parameter of a transfer rule is randomly chosen before each transfer of the N-byte data element, with the transfer rule defining the order in which the bytes of the N-byte data element are transferred through the data bus. The N-byte data element is transferred byte-by-byte through the data bus in the order specified by the transfer rule, with each byte transiting once and only once through the data bus.

Because the value of at least one parameter of the transfer rule is randomly chosen before each transfer of the N-byte data element, the bytes of the data element are not transferred in the same order for each transfer of that data element. This makes the simple power analysis method of snooping no longer sufficient to obtain the value of the data element transiting through the data bus.

The Pfab reference is directed to a data processing circuit in which the data transiting on the data bus and stored in memory is protected by being encoded. However, Pfab does not disclose a method for secured transfer of an N-byte data element in which the value of at least one parameter of a transfer rule that defines the order in which the bytes of the data element are transferred is randomly chosen before each transfer of the data element, and the N-byte data element is transferred byte-by-byte in the order specified by the transfer rule, as is recited in amended claim 1. Amended claim 14 contains similar recitations.

Likewise, Pfab does not disclose a programmable circuit that includes a random number generator that supplies the value of at least one parameter of a data transfer rule that defines the order in which the bytes of the data element are transferred before each transfer of the data element, and a control unit that controls a data bus such that the N-byte data element is transferred byte-by-byte in the order specified by the data transfer rule, as is recited in amended claim 22.

Pfab discloses a data processing circuit in which data is stored in memory and transferred through the data bus in an encoded format. In the first and second embodiments, the data processing circuit includes a microprocessor 101, a data bus 106, and memories 102-105, as shown in Figures 1 and 2. Each memory 102-105 stores encoded data, and this encoded data is transferred through the data bus 106. The microprocessor 101 includes an encoding module 107

that decodes the encoded data received from the data bus 106, and encodes data to be sent each memory 102-105 through the data bus 106.

In the third embodiment, the data processing circuit includes a microprocessor 1, data buses 6-15, and memories 2-5, as shown in Figure 3. Each memory 2-5 stores encoded data, and this data is transferred through the data buses 6-15 at least partially encoded. The microprocessor 1 includes one encoding module 35 and an additional encoding module 20-22 is provided on the data buses 6-15 between each memory 2-5 and the microprocessor 1. The encoded data stored in each memory 2-5 is partially decoded by the associated encoding module 20-22 and then completely decoded by the encoding module 35 of the microprocessor. Similarly, data sent to each memory 2-5 is partially encoded by the encoding module 35 of the microprocessor and then completely encoded by the associated encoding module 20-22. Thus, Pfab teaches data processing circuits in which data is protected by modifying (i.e., encoding) each byte of data stored in memory and transferred through the data bus.

In contrast, in embodiments of the present invention, an N-byte data element is securely transferred byte-by-byte by using a transfer rule having one or more parameters whose values are chosen at random so that the bytes of the data element are not transferred in the same order for each transfer of that data element. More specifically, a transfer rule defines the order in which the bytes of the N-byte data element are transferred through the data bus, and the value of one or more parameters of the transfer rule are randomly chosen before each transfer of the N-byte data element. The N-byte data element is transferred byte-by-byte through the data bus in the order specified by the transfer rule, with each byte transiting once and only once through the data bus. For example, in one embodiment a random number generator supplies the value of the one or parameters of the data transfer rule before each transfer of the N-byte data element, and a control unit controls the data bus such that the N-byte data element is transferred byte-by-byte through the data bus in the order specified by the data transfer rule.

Because the value of one or more parameters of the transfer rule are randomly chosen before each transfer of the N-byte data element, the bytes of the data element are not transferred in the same order for each transfer of that data element. This makes the simple power analysis method of snooping no longer sufficient to obtain the value of the data element transiting through

the data bus. Thus, in embodiments of the present invention, data is protected by modifying the order in which the bytes of a data element are transferred, not by modifying the data itself. In other words, regardless of whether the data is stored in memory and transferred in clear or encoded format, the order of transfer of the bytes is modified.

Pfab does not teach or suggest a circuit or method for securely transferring an N-byte data element in which the value of at least one parameter of a transfer rule that defines the order in which the bytes of the data element are transferred is randomly chosen before each transfer of the data element, and the N-byte data element is transferred byte-by-byte in the order specified by the transfer rule. While Pfab does teach using a random number generator in selecting which of the keys to use to encode the data, Pfab does not teach or suggest using the random number generator in choosing the value of one or more parameters of a transfer rule that defines the order in which the bytes of the data element are transferred.

Similarly, while Pfab does suggest using a permutation to encode the data, Pfab does not teach or suggest using a permutation of the bytes of an N-byte data element such that each transfer of the N-byte data element is not done in the same byte order. Pfab does not teach or suggest modifying the order of the transfer of the bytes of an N-byte data element, let alone teach or suggest doing so by randomly choosing the value of one or more parameters of a data transfer rule that defines the order in which the bytes of the data element are transferred.

Applicant believes that the differences between Pfab and the present invention are clear in amended claims 1, 14, and 22, which set forth various embodiments of the present invention. Therefore, claims 1, 14, and 22 distinguish over the Pfab reference, and the rejection of these claims under 35 U.S.C. § 103(a) should be withdrawn.

As discussed above, amended claims 1, 14, and 22 distinguish over the Pfab reference. Furthermore, the claimed features of the present invention are not realized even if the teachings of Menezes are incorporated into Pfab. Menezes does not teach or suggest the claimed features of the present invention that are absent from Pfab. Thus, claims 1, 14, and 22 distinguish over the Pfab and Menezes references, and thus, claims 2-13, claims 15-21, and claims 23 and 24 (which depend from claims 1, 14, and 22, respectively) also distinguish over the Pfab reference.

Therefore, it is respectfully submitted that the rejections of claims 1-24 under 35 U.S.C. § 103(a) should be withdrawn.

In view of the foregoing, it is respectfully submitted that the application and the claims are in condition for allowance. Reexamination and reconsideration of the application, as amended, are requested.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is invited to call the undersigned attorney at (561) 989-9811 should the Examiner believe a telephone interview would advance the prosecution of the application.

Respectfully submitted,

Date: December 3, 2004

By: _____

Stephen Bongini
Registration No. 40,917
Attorney for Applicant

FLEIT, KAIN, GIBBONS,
GUTMAN, BONGINI & BIANCO P.L.
One Boca Commerce Center
551 Northwest 77th Street, Suite 111
Boca Raton, Florida 33487
Telephone: (561) 989-9811
Facsimile: (561) 989-9812